

REMARKS

The applicant thanks Examiner Zia for taking time out of his schedule to attend the telephone interview held on June 23, 2009 with the applicant's representatives, Mr. Jeffrey J. Barclay (Reg. No. 48,950) and Ms. Yina Mo. During the interview, the pending claims were discussed along with the U.S. Patent No. 6,718,468 to Challener et al. Portions of this reply have been prepared based upon the discussion.

Claims 1-10 are currently pending with claims 1 and 7 being independent. Claims 1-10 have been amended and no new matter has been entered by way of these amendments. Favorable reconsideration and further examination of the action mailed on February 5, 2009 is respectfully requested in view of the following comments of the Applicant, which are proceeded by related comments of the Examiner in small bold type.

Claims 1-10 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Not conceding to the Examiner's position, claims 1-10 have been amended. Claims 1-6 have been amended to recite a computer-implemented method, and claims 7-10 have been amended to recite a computer-executable program.

Claims 1-10 are rejected under 35 U.S.C. 102(e) as being anticipated by Challener et al. (U.S. Patent 6,718,468).

Challener does not describe and would not make obvious "generating a first key from a user-supplied unencrypted password," and "encrypting the user's password with the first key," as recited by amended independent claim 1.

In contrast, Challener is understood to describe an encryption technique that uses a pre-existing public key (referred to as a chip public key) to encrypt three types of information (i.e., a user public/private key pair, a random password, and a first password). However, Challener's public key used for encrypting is completely unrelated to the information being encrypted. In particular, the chip public key has no connection whatsoever to the key pair (i.e., the user

public/private key pair) or the passwords (i.e., the random password or the first password). As such, the reference does not describe or suggest, generating a first key from a user-supplied unencrypted password, and encrypting the user's password with the first key, as required by claim 1.

While Challenger's chip public key is produced at some point, the reference appears silent regarding the production of the chip public key and simply states that the chip public key is provided from storage on a chip (referred to as a signature chip). In particular, the reference reads:

The chip public key may come from an unprotected or protected storage area of the signature chip. (column 4, lines 22-23)

Challenger appears to describe the production of the information being encrypted. For example, the random password is produced by a random generator (column 4, lines 17-20) and the first password is produced by hashing a pass phrase provided a user (column 4, lines 30-31 and 42-43). Similarly, the public/private key pairs are established by computer applications (column 3, lines 55-57). As such, the information being encrypted is not used to produce the public chip key, which is used to encrypt the information.

Furthermore, Challenger does not describe a user providing the data to be encrypted (i.e., the public/private key pairs, the random password and the first password). While the reference mentions that a pass phrase is provided by a user (column 4, lines 42-43), this pass phrase is not encrypted but is simply used to generate the first password.

Thus, Challenger does not describe and would not make obvious "generating a key from a user-supplied unencrypted password," and "encrypting the user's password with the key". Accordingly, the applicant asserts that Challenger does not anticipate the features of independent claim 1 and the claim is patentable.

Amended independent claim 7 includes subject matter similar to claim 1, and is patentable for at least reasons similar to those described for claim 1. Claims 2-6 and 8-10 respectfully depend upon independent claims 1 and 7, and all of these dependent claims are

patentable for at least similar reasons as those for the claims on which they depend are patentable. Canceled claims, if any, have been canceled without prejudice or disclaimer.

Any circumstance in which the applicant has (a) addressed certain comments of the Examiner does not mean that the applicant concedes other comments of the Examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the Examiner's positions with respect to that claim or other claims.

The required fee in the amount of \$245 for the Petition for Extension of Time is being paid concurrently herewith on the Electronic Filing System (EFS) by way of Deposit Account Authorization. Please apply any other charges or credits to deposit account 06-1050, referencing Attorney Docket No.: 13984-0005US1.

Respectfully submitted,

Date: 6 July 2009



Jeffrey J. Barclay
Reg. No. 48,950

Fish & Richardson P.C.
Telephone: (617) 542-5070
Facsimile: (877) 769-7945